Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

An unending variety of topics

Friday, August 18, 2006

Finding jammers in a DC network

David Chaum's dining cryptgraphers network is a nifty alternative to his digital mix to untraceably share encrypted information. But it suffers from the problem that since the participants are untraceable, one or more of them can jam the channel, preventing other participants from having their messages received. Bryan Turner has figured out a way to find the jammers if they are less than one-third of the total participants. Presumably this is accomplished without being able to find out much of anything else interesting about a participant. I suggest that a similar technique may also work for a jamming attack in a secure multiparty computation.

Posted by Nick Szabo at 10:07 AM

Newer Post Home Older Post

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ► 2007 (47)
- ▼ 2006 (130)
  - ► December (4)
  - ► November (7)
  - ► October (15)
  - ► September (15)
  - ▼ August (20)
    - Drinking and lawyering don't mix
    - How to become a dictator in a democracy
    - Why the housing inflation?
    - "Do you think government is too big, too powerful?...
    - Pollution reduction with cap & trade
    - Colliding galaxy clusters show dark matter
    - Patents: the coming obviousness showdown
    - Colonialism just ain't what it used to be
    - What was the Coalition Provisional Authority?
    - A disturbing new beast
    - Conservation of rights
    - Limits on the income tax
    - From parody to politics

Psychological pricing and mental transaction costs...

The return of human uniqueness?

Smart contracts, tying, and product liability

Finding jammers in a DC network

Book consciousness

Charters and judicial review

Smart contracts in pieces

► July (5)

► June (10)

► May (4)

► April (3)

► March (11)

► February (10)

► January (26)

► 2005 (44)

Simple theme. Powered by Blogger.